

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

16 03/27 20
Rec'd PCT/PTO 27 DEC 2004
IB 03/27 20

Intyg Certificate

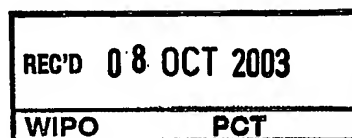
Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) Sökande ABB AS, Billingstad NO
Applicant (s)

(21) Patentansökningsnummer 0202019-6
Patent application number

(86) Ingivningsdatum 2002-06-28
Date of filing



Stockholm, 2003-09-30

För Patent- och registreringsverket
For the Patent- and Registration Office

Kerstin Gerdén
Kerstin Gerdén

Avgift
Fee 170:-

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2002-05-14
4-9432SE/LG

Revalidation of a compiler for safety control

5 TECHNICAL FIELD

The present invention concerns revalidation of a compiler of control language for use in an industrial control system. In particular the invention reveals a method to revalidate a compiler for compilation of a user written program, which is intended for safety control of real world entities. The user written program subject to compilation by the compiler is intended for execution in a device, which comprises functionality that adds safety features to an industrial control system. The invention insures that no fault is introduced into the device due to error in the compiler code. Such an error can for instance occur during distribution of the compiler code. An error can also occur due to failure in a computer's memory or on a disk where the compiler code is stored.

20 The invention insures that no such fault is introduced into the control of real world entities which otherwise could lead to accidents that harm people or cause damage to the environment.

25 BACKGROUND ART

Industrial control systems are for instance applied in manufacturing and process industries, such as chemical plants, oil production plants, refineries, pulp and paper mills, steel mills and automated factories. Industrial control systems are also widely used within the power industry. Such industrial control systems may need to comprise or be combined with devices, which adds safety features. Example of processes which requires additional safety features than what a standard industrial control

system provides are processes at off-shore production platforms, certain process sections at nuclear power plants and hazardous areas at chemical plants. Safety features may be used in conjunction with safety shutdown, fire and/or alarm systems as well as for fire-and-gas detection.

An example of an industrial control system, which includes a safety critical function, is described in DE19857683 "Safety critical function monitoring of control systems for process control applications has separate unit". The system has a main controller bus coupled to different processors via a number of decentralized data receivers.

The use of general-purpose computer systems raises issues in that a user written program do not get affected by a fault in the compiler code.

"Compilers: Principles, techniques and tools" by Alfred V. Aho, Ravi Sethi and Jeffrey D. Ullman published 1988 by Addison-Wesley publishing company, includes a discussion on verification of general-purpose compilers. Page 731 paragraph 11.4 "Testing and maintenance" handles the verification of compilers according to standard software testing. One approach, suggested in the book, is the "regression" test. A suite of test programs is maintained, and whenever a compiler is modified, the test programs are compiled using both the new and old version of the compiler. Any difference in the target programs produced by the two compilers is reported to the compiler writer. Further the book points out that choosing the

programs to include in a test suite is a difficult problem.

Prior art in the area of compilation technology include
 5 methods and systems for compiler optimization. US5577253
 "Analyzing inductive expressions in a multilanguage
 optimizing compiler" describes a method executed in a
 computer system where a plurality of optimizations is
 performed by a generic compiler back-end using induction
 10 variables. This patenting optimization technique does not
 address the correctness of a compiler at a later time.

US6071316 "Automated validation and verification of
 computer software" shows a method for verifying that a
 15 source code, which has been compiled, executes all
 different paths in the code. This is not concerned with
 the compiler correctness.

A remaining problem in the area of safety control of real
 20 world entities is to insure the highest possible
 reliability of a user written program.

Another problem relating to industrial control systems is
 that the complexity of system software distribution (such
 25 as via Internet) has led to an increased risk of that
 errors occurs in the compiler software.

The inventors have found that there is a need to ensure
 that a compiler for software with the purpose of safety
 30 control of real world entities do not change it's way to
 produce code during that it is distributed, stored as
 binary code or is recompiled from the associated high
 level code.

SUMMARY OF THE INVENTION

An object of the present invention is to provide a method to revalidate a compiler intended for compilation of a user written program for execution of safety control in an industrial control system.

This and other objects are fulfilled by the present invention according to a method described in a claim 1. Advantageous embodiments are described in sub-claims.

With the present invention a test program, defined in a control language, is compiled. By verifying that the test program executes correctly, the compiler is validated. A first software means for later comparison purposes is generated. In conjunction with the compilation of a user written program the test program is compiled. Based on the second compilation of the test program a second software means is generated. The compiler is revalidated for errors introduced between the first and second compilation by comparing the first and second software means. Provided that the revalidation indicates no errors in the compiler, the user written program is enabled to execute in a device with safety features for control of real world entities.

The user written program subject to compilation by the compiler is intended for execution in a device, which comprises functionality that adds safety features to an industrial control system. As mentioned above a method according to the invention include steps which shows how to generate a first and second software means based on a compiled test program. Typically the first software means

is generated at the time of establishing of new version or revision of the compiler of a control language. The first software means is typically associated with the revision or version of the compiler code at hand. The method comprises steps where a second software means is generated at the time of compilation of a user written program. The method comprise steps in which the first and second software means are used to revalidate the compiler by comparing the first software means with the second software means. The first software means and the second software means are derived from the compiled test program by use of the same principals.

The invention facilitates that no fault is introduced into the industrial control system due to error in the compiler code. Such an error can for instance occur during distribution of the compiler code or an error can be due to failure in a computer's memory or failure in a disk where the compiler code is stored. An error in the compiler code can also occur due to faults in a computer register, a stack memory or in a CPU.

A particular useful feature of the invention is that it facilitates that no such fault is introduced into the device for safety control of real world entities which otherwise could lead to accidents that harm people or cause damage to the environment.

The user written program is typically written in control language, for instance based on IEC 61131-3.

An aim of the invention is to detect a fault in the compiler code. The invention detects errors in the

compiler code at any time of compilation, which insures a high reliability of safety critical user written program compiled by the said compiler.

- 5 A further object of the invention is to provide a computer program product containing software code means loadable into the internal memory of a general-purpose computer or workstation and/or a device, which computer program products has software means to execute at least
10 one step of the above described method.

Yet a further object of the invention is to provide a computer program comprising computer code means and/or software code portions for making a computer or processor
15 perform any of the steps of the above described method.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described in more detail in connection with the enclosed schematic drawings.

20

Figure 1 shows a schematic overview of an industrial control system comprising a computer loaded with compiler code and a device with safety control features.

Figure 2 shows a schematic flowchart of a method based on
25 the invention.

Figure 3 shows a simplified diagram of an embodiment of the invention in where the compilation of the test program is performed at the same time as the compilation of a user written program. The compiled test program is
30 compared with a previous compilation of the test program.

Figure 4 shows a simplified diagram of another embodiment of the invention where the compilation of the test program is performed at the same time as the compilation

5

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 shows a schematic diagram of an industrial control system 2 with a device 6a comprising safety features 6b. A user written program intended for safety

5 control of real world entities 10 is typically compiled in a workstation 5a or in a general purpose computer.

Such a workstation 5a or general purpose computer is connected by communication means 3 to the device 6a. The communication means 3 is based on communication standards

10 such as fieldbus technology or such as TCP/IP. The industrial control system 2 comprise a multitude of different devices such as controllers 6c, PLCs 7,

operator stations or process portals 4 and process I/O 8.

The above mentioned devices may exist in any number and
15 in combination with other devices common in an industrial control system. The device 6a comprising safety features

6b may be an individual device such as a PLC or controller. The safety features are such that the device and/or the industrial control system comply with safety

20 standards such as Safety Integrity Levels (SIL) as defined in the standard IEC 61508. The device may also comprise one or several software modules with safety features added to the device. The device 6a is connected

to real world entities 10 subject to safety control via
25 communication means such as a fieldbus or process I/O.

Examples of real world entities are actuators, instruments, motors, valves, pumps, fans etc. A real world entity may also be a group of entities or a system of entities.

30

A device 6a for safety applications in a process control system 2 typically execute user written applications described in a high level language derived from the

standard IEC 61131-3, which is well known to a person skilled in the art. Hence, the compiler 22 is typically a compiler for a high level language derived from the standard IEC 61131-3.

5

Hereafter a release, a version or a revision of the compiler is called the compiler.

10 Validating a compiler for safety control is typically made at a software factory. A software factory is in this context a location where sufficient and certified test equipment as well as qualified personal is available to perform tests and validation of the compiler. Validation of the compiler and the associated tests should be
15 substantial. The tests should for instance insure that the compiler 22 and the safety features meet requirements of safety certification. Also other requirements need to be met such as sufficient performance in order for other applications or programs to execute in the industrial
20 control system 2. The validation of the compiler comprise verification of that applications executes correctly in the device for safety control of real world entities.

The invention disclose that, in addition to the above
25 described validation of a compiler, a test program 20 is established where the purpose of the test program 20 is to use it as input for revalidation of the compiler 22 outside the software factory. A test program 20 should include all logic of the control language, which is used
30 for safety control applications. The definitions used in a typical test program are typically derived from the IEC 61131-3 standard. A preferred test program is built by using all languages, all functions and all language

constructs. This in order to insure that the compiler 22
parses and checks all logic expressions during
compilation of the test program which later are to be
used in a user written program 21.

5

In an embodiment of the invention a version or revision
of the compiler from the software factory is associated
with the test program. The test program is at least
partly used in the validation of the compiler at the
10 software factory. A first software means intended for
later comparison purposes is also associated with the
version or revision of the compiler. It is further
advantageous to distribute the test program together with
the release, version or revision of the compiler.

15

Figure 2 shows a schematic flow chart of a method based
on the invention. The test program 20 is defined in a
control language. The method comprises the step of
compiling 11a the test program by means of the compiler.
20 Further the method comprises the step of validating 11b
the compiler by verification of that the test program
executes correctly.

Figure 2 also shows that the method comprises the step of
25 generating a first software means 12. The first software
means is dependant of the executable code of the test
program 20. The first software means may have many
embodiments. In one embodiment the first software means
23 comprise the original executable code of the compiled
30 test program. In another embodiment generating 12 a first
software means comprise the calculation of a check-sum
and/or a code for cyclic redundancy check. In such an
embodiment the check-sum and/or the code for cyclic

redundancy check is calculated with the compiled test program as one input. Hereafter a code for cyclic redundancy check is called CRC. A CRC can be calculated or derived in several ways. For instance, a CRC can be of length 16 bit or 32 bit. The 16 bit polynomial CRC-CCITT ($X^{16}+X^{12}+X^5+1$) or the 16 bit polynomial ($X^{16}+X^{15}+X^2+1$) are example of polynomials suitable to be used in embodiments of the invention. An example of a 32 bit polynomial, which can be used to calculate a CRC, is

10 ($X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$). The mentioned 32 bit polynomial is defined in the Ethernet standard IEEE 802.3 and is a preferred polynomial to use in embodiments of the invention. In an alternative embodiment a checksum, such as a parity check, could be

15 used.

Figure 2 shows that a method based on the invention comprises the step of compiling 13 the test program 20 a second time. Compiling 13 the test program 20 is made in conjunction with the compilation of a user written program 21. The time lag between generating 12 the first software means 23, 35 and compiling 13 the test program 20 a second time, is typically, several days or weeks. The time lag may be up to several years. During the time

25 between generating 12 the first software means and compiling 13 the test program a second time, an error in the compiler code might have occurred. Such an error can for instance occur during distribution of the compiler code or an error can be due to failure in a computer's memory or failure in a disk where the compiler code is

30 stored. An error in the compiler code can also occur due to faults in a computer register, a stack memory or in a CPU.

Further, figure 2 shows that the method comprises the step of generating 14 a second software means 24a, 31 based on the second compilation of the test program 20. The step of generating the second software means 24a, 31 is based on the same principals as the previous step of generating 12 the first software means. As with the first software means the second software means may have many embodiments. In one embodiment the second software means 24a comprise the executable code of the second compilation of the compiled test program 20. In another embodiment generating 14 the second software means comprise a calculation of a check-sum and/or a code for cyclic redundancy check. Alternative ways of calculation a check-sum and/or a code for cyclic redundancy check are described in more detail in the above description of generating the first software means. Figure 3 shows a more detailed overview of generating 14 a second software means 24a and the following steps of comparing 15 software means and enabling 16 the user written program 26. Figure 4 indicates that in an alternative embodiment of the invention the second software means 31 is downloaded to the device 6a.

Figure 2 also shows that the method comprises the step of comparing 15 the first software means with the second software means. Figure 3 shows that in one embodiment of the method the comparing step is performed by means of the same workstation 5a or general purpose computer as in which the compiler 22 is installed. In such embodiment the comparing step 15 of the first software means 23 and the second software means 24a may be implemented by use of standard features provided by an operating system.

In another embodiment the comparing step 15 is performed by means of the device 6a. Figure 4 shows an overview of

such an embodiment. In such an embodiment it is preferable that the first software means 35 is down-loaded to the device 6a together with the system software. Figure 4 indicates that the first software means 35 typically has been down-loaded to the device 6a before the second compilation of the test program 20. The second software means 31 is down-loaded 34 in conjunction with a successful compilation of the user written program 26.

Comparing 15 the software means does, in one embodiment of the invention, involve a compare of the reminder values - and not between the values where the reminder is included in the calculation. In the latter case the value will be 0 and a comparison between 0 and 0 may result in that the stored calculation is placed in a memory where some or all bits are stuck at 0 and the comparison may give an invalid result. That is why a comparison between nonzero values (such as reminder values) yields a higher probability to discover faults.

In an alternative embodiment of the invention the steps of compiling the test program 13, generating 14 a second software means and comparing 15 the first and second software means is repeated any number of times. In such an alternative embodiment an additional source of data may be used with the purpose of generating a change in both the first and second software means. An example of such an embodiment is that the generating step of the second software means comprise an additional step of combining a variable that change over time with the second software means. The variable that change over time typically relates to the second compilation of the test program. In the same alternative embodiment the comparing step may comprise an additional step of down-loading the variable that change over time. It is advantageous to use a date&time stamp. In one embodiment according to figure 4 the date&time stamp is down-loaded to the device 6a and

the date&time stamp is combined with the first software means 35. The advantage of using a variable that change over time, such as a date&time stamp, is to generate a change in the first and second software means over time.

- 5 Such a change eliminates the possibility that one unit in the down-load chain, stores the second software means during a down-load and at a later down-load sends that second software means instead of the new one it receives.
- 10 Figure 2 also shows that the method comprise the step of enabling 16 the compiled user written program 26 to execute in the device 6a with safety features for control of real world entities 10. The enabling step of the method is performed provided that no errors were detected
- 15 in the compiler in the previous steps.

A method according to the invention is at least partly performed under control of a set of computer readable instructions contained in a computer program storage

20 device.

- The invention also discloses a computer program product 5b intended for safety control in an industrial control system 2. The computer program product 5b comprise
- 25 functionality of enabling a user written program to execute after revalidating the compiler according to the above described methods. Further the computer product comprises software means for carrying out a further action to receive a signal sent across internet 1
- 30 comprising the first software means 35.

The invention also discloses a computer program comprising computer code means for making a computer or processor perform any of the steps of the above described

35 method.

The foregoing disclosure and description of the invention are illustrative and explanatory thereof, and various changes in the components, processing and computational steps and procedures, as well as in the details of the illustrated circuitry and method of operation may be made without departing from the spirit of the invention.

1
2
3
4
5
6
7
8
9
10

CLAIMS

1. A method to revalidate a compiler (22) intended for compilation of a user written program for safety control in an industrial control system (2), comprising the steps of
- compiling (11a) a test program (20) a first time which test program is defined in a control language;
 - validating (11b) the compiler by verification of that the test program executes correctly;
 - characterized by the further steps of
 - generating (12) a first software means derived from the compiled test program intended for later comparison purposes;
 - compiling (13) the test program a second time in conjunction with the compilation of a user written program;
 - generating (14) a second software means intended for a comparison based on the second compilation of the test program;
 - comparing (15) the first software means with the second software means; wherein the compiler (22) is revalidated for errors introduced between the first and the second compilation;
 - enabling (16), provided that the revalidation indicates no errors in the compiler (22), the user written program to execute in a device (6a) with safety features for control of real world entities (10)..
2. A method according to claim 1, characterized in that the comparing step (15) is performed in the same workstation (5a) or general-purpose computer as the compiler (22) is executing.

3. A method according to claim 1, characterized in that the software means is a check-sum or a code for cyclic redundancy check.

5 4. A method according to claim 3, characterized in that the comparing step (15) is performed in the device (6a) with safety features.

10 5. A method according to claim 4, characterized in that the comparing step (15) comprise an additional step of down-loading a variable that change over time, which is down-loaded in the same message as the check-sum or code to the device (6a), where the variable that change over time is used to achieve a change in the message.

15

6. A method according to claim 1, characterized in that the test program (20) is defined in a control language derived from the standard IEC 6-1131.

20 7. A computer program product (5b) containing software code means loadable into the internal memory of a general-purpose computer or workstation (5a) and/or a device (6a), characterized in that said computer program product has means to execute a computer implemented step
25 of compiling (13) the test program a second time, a computer implemented step of generating a second software means (14), a computer implemented step of comparing (15) the first software means with the second software means and a computer implemented step of enabling (16) the user
30 written program to execute in the device (6a), all steps according to claim 1.

8. A computer program product (5b) according to claim 7 which comprise software means for carrying out a further action to:

5 -receive a signal sent across internet (1) comprising the first software means (35).

9. A computer program comprising computer code means and/or software code portions for making a computer or processor perform any of the steps of claims 1-6.

10

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
219

ABSTRACT

The present invention concerns revalidation of a compiler of control language for use in an industrial control system. In particular the invention reveals a method to

5 revalidate a compiler for compilation of a user written program, which is intended for safety control of real world entities. The user written program subject to compilation by the compiler is intended for execution in a device, which comprises functionality that adds safety

10 features to an industrial control system. The invention insures that no fault is introduced into the device due to error in the compiler code. Such an error can for instance occur during distribution of the compiler code or due to failure in a computer's memory or failure on a

15 disk where the compiler code is stored. Hence the invention insures that no such fault is introduced into the control of real world entities which otherwise could lead to accidents that harm people or cause damage to the environment.

20

Fig. 2

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

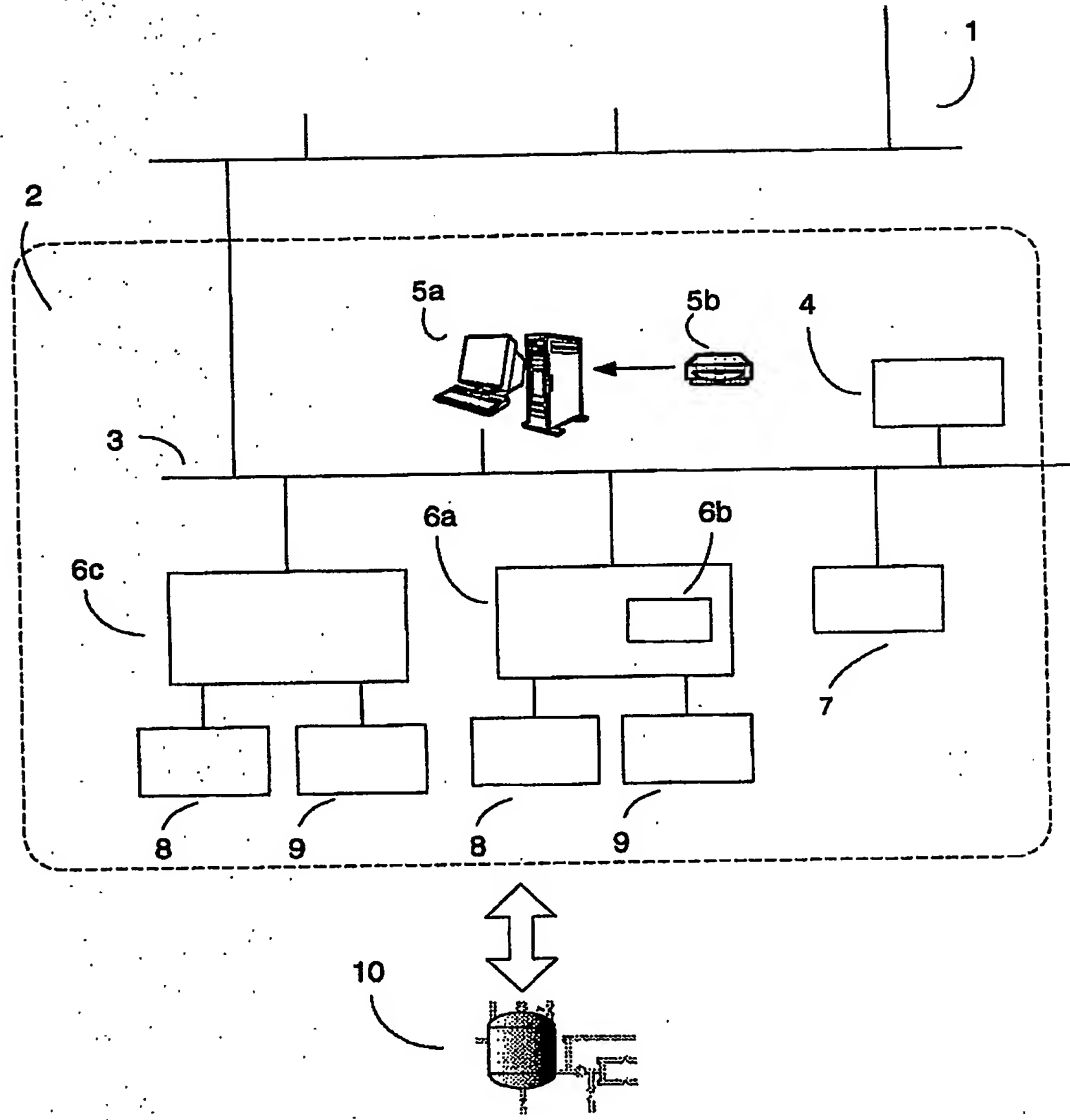


Fig. 1

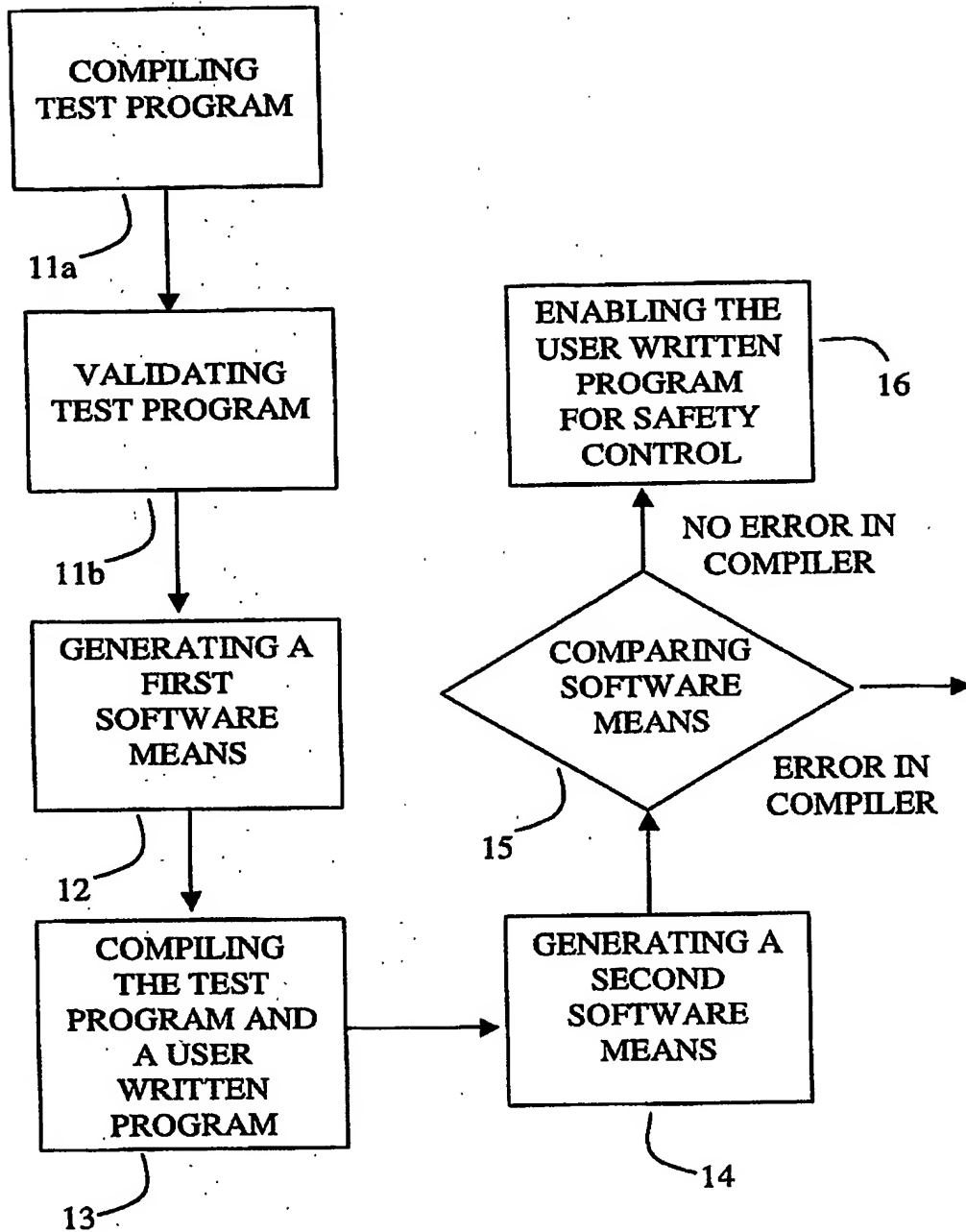


Fig. 2

3/4

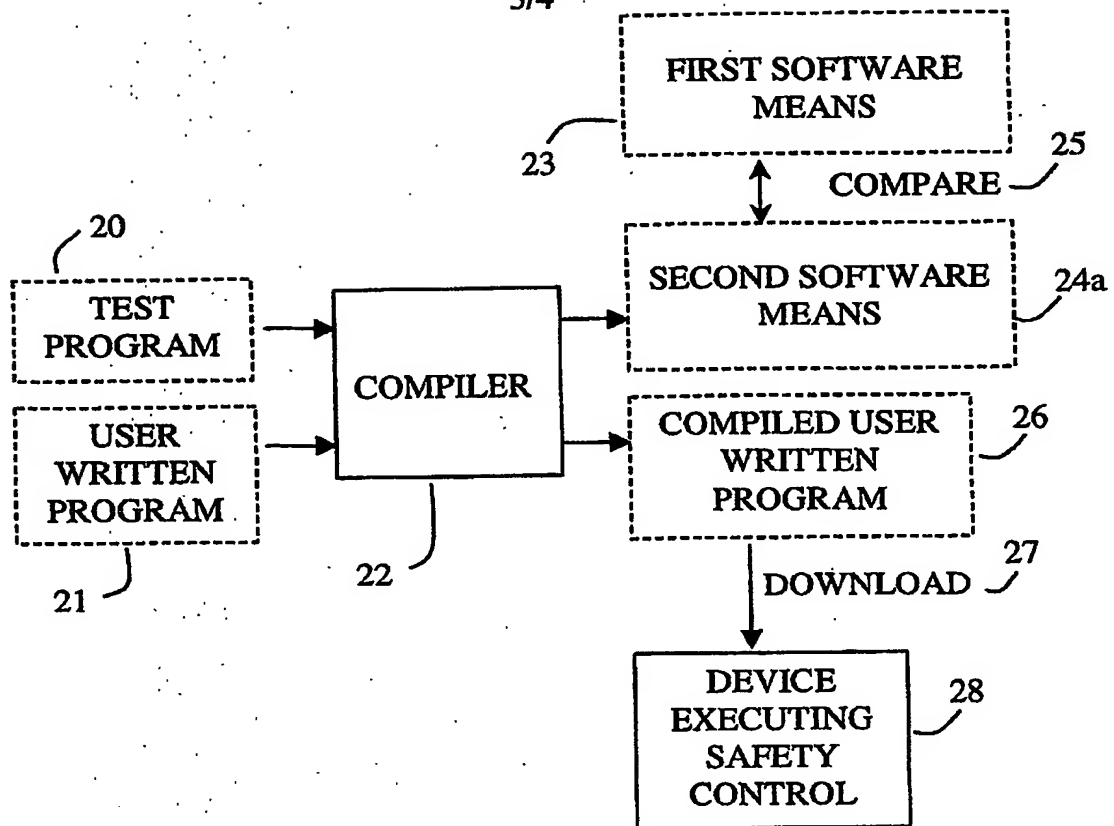


Fig. 3

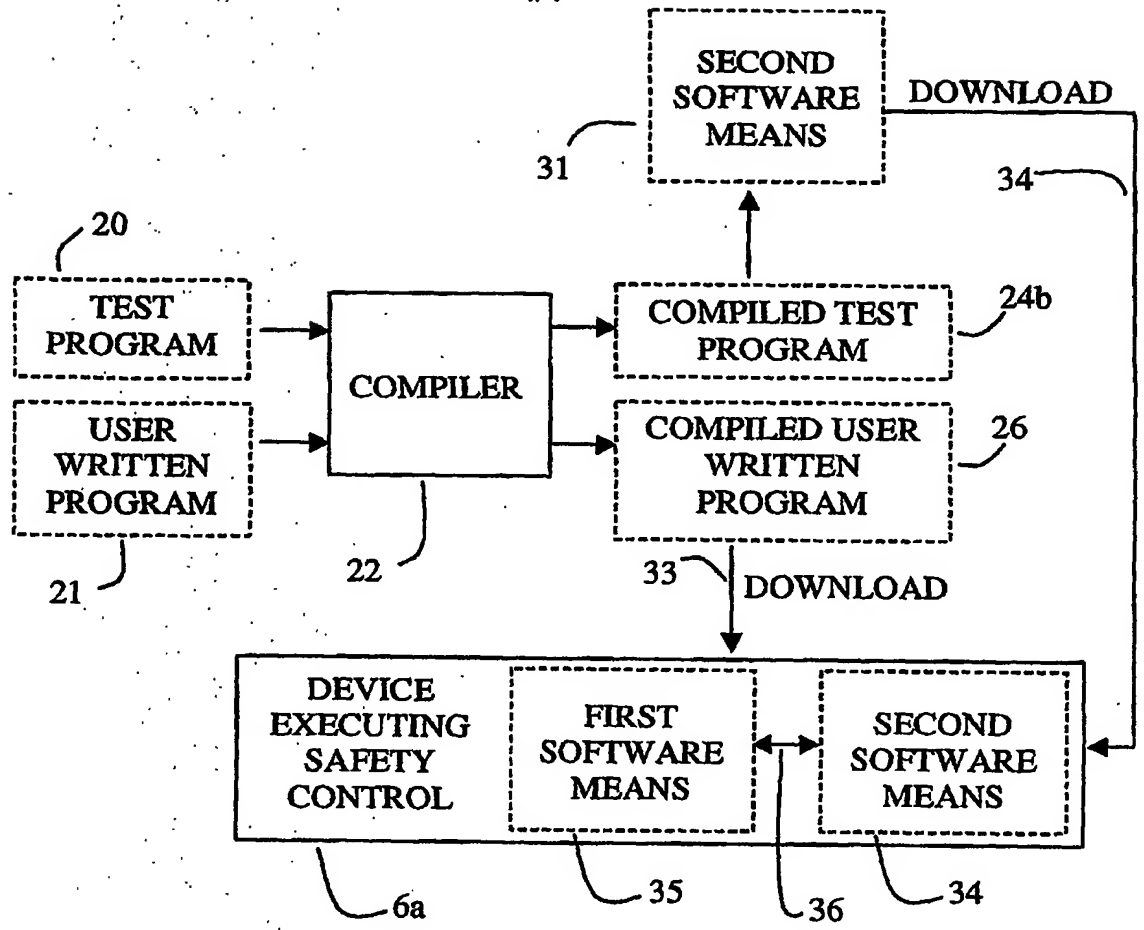


Fig. 4